PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) **Classification internationale des brevets** 6 : **H04N 7/16**

A1

(11) **Numéro de publication internationale:** **WO 99/57901**

(43) **Date de publication internationale:** 11 novembre 1999 (11.11.99)

(21) **Numéro de la demande internationale:** PCT/IB99/00821

(22) **Date de dépôt international:** 6 mai 1999 (06.05.99)

(30) **Données relatives à la priorité:**
PCT/IB98/00681 7 mai 1998 (07.05.98) IB

(71) **Déposant** *(pour tous les Etats désignés sauf US)*: KUDELSKI S.A. [CH/CH]; 22, route de Genève, CH–1033 Cheseaux–sur–Lausanne (CH).

(72) **Inventeurs; et**
(75) **Inventeurs/Déposants** *(US seulement)*: KUDELSKI, André [CH/CH]; Chemin de Bellingard, CH–1095 Lutry (CH). SASSELLI, Marco [CH/CH]; 20, chemin des Roches, CH–1803 Chardonne (CH).

(74) **Mandataire:** GRIFFES CONSULTING S.A.; 81, route de Florissant, CH–1206 Genève (CH).

(81) **Etats désignés:** AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, brevet ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

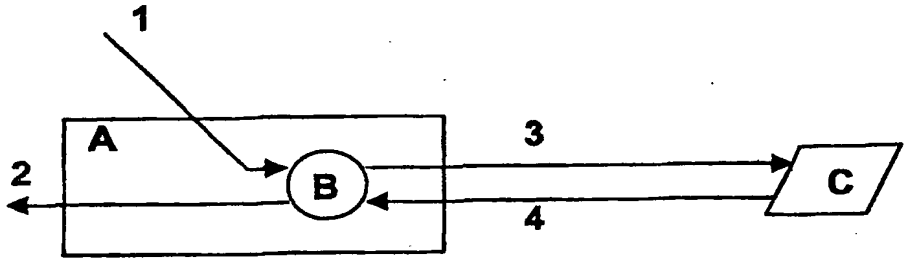
Publiée
Avec rapport de recherche internationale.

(54) **Title:** MECHANISM FOR MATCHING A RECEIVER WITH A SECURITY MODULE

(54) **Titre:** MECANISME D'APPARIEMENT ENTRE UN RECEPTEUR ET UN MODULE DE SECURITE

(57) **Abstract**

The invention concerns a system for controlling data transmission between a receiver and a security module, in particular for a pay television system, wherein the transmitted data are encrypted and decrypted by means of an encryption key, stored in the receiver and in the security module.



(57) **Abrégé**

Système de contrôle de transmission d'informations entre un récepteur et un module de sécurité, notamment pour un système de télévision à péage, où les informations transmises sont chiffrées et déchiffrées au moyen d'une clé de chiffrement unique, stockée d'une part dans le récepteur, et d'autre part dans le module de sécurité.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie
AM	Arménie
AT	Autriche
AU	Australie
AZ	Azerbaïdjan
BA	Bosnie-Herzégovine
BB	Barbade
BE	Belgique
BF	Burkina Faso
BG	Bulgarie
BJ	Bénin
BR	Brésil
BY	Bélarus
CA	Canada
CF	République centrafricaine
CG	Congo
CH	Suisse
CI	Côte d'Ivoire
CM	Cameroun
CN	Chine
CU	Cuba
CZ	République tchèque
DE	Allemagne
DK	Danemark
EE	Estonie
ES	Espagne
FI	Finlande
FR	France
GA	Gabon
GB	Royaume-Uni
GE	Géorgie
GH	Ghana
GN	Guinée
GR	Grèce
HU	Hongrie
IE	Irlande
IL	Israël
IS	Islande
IT	Italie
JP	Japon
KE	Kenya
KG	Kirghizistan
KP	République populaire démocratique de Corée
KR	République de Corée
KZ	Kazakstan
LC	Sainte-Lucie
LI	Liechtenstein
LK	Sri Lanka
LR	Libéria
LS	Lesotho
LT	Lituanie
LU	Luxembourg
LV	Lettonie
MC	Monaco
MD	République de Moldova
MG	Madagascar
MK	Ex-République yougoslave de Macédoine
ML	Mali
MN	Mongolie
MR	Mauritanie
MW	Malawi
MX	Mexique
NE	Niger
NL	Pays-Bas
NO	Norvège
NZ	Nouvelle-Zélande
PL	Pologne
PT	Portugal
RO	Roumanie
RU	Fédération de Russie
SD	Soudan
SE	Suède
SG	Singapour
SI	Slovénie
SK	Slovaquie
SN	Sénégal
SZ	Swaziland
TD	Tchad
TG	Togo
TJ	Tadjikistan
TM	Turkménistan
TR	Turquie
TT	Trinité-et-Tobago
UA	Ukraine
UG	Ouganda
US	Etats-Unis d'Amérique
UZ	Ouzbékistan
VN	Viet Nam
YU	Yougoslavie
ZW	Zimbabwe

MECANISME D'APPARIEMENT

ENTRE UN RECEPTEUR ET UN MODULE DE SECURITE

DOMAINE TECHNIQUE

Cette invention se rapporte à un système de contrôle de transfert d'informations entre un récepteur et un module de sécurité, notamment pour un système de télévision à péage, ainsi qu'à une méthode de contrôle du transfert d'informations brouillées.

ARRIERE-PLAN DE L'INVENTION

Un système de débrouillage de télévision à péage est composé d'un récepteur et d'un module de sécurité. Ce module peut être détachable ou fixe. Le récepteur a pour mission de débrouiller les signaux reçu. Le module de sécurité a pour mission principale de contrôler l'opération en vérifiant l'autorisation de débrouillage et en fournissant, le cas échéant, les informations nécessaires au fonctionnement du module de débrouillage, par exemple par la fourniture de vecteurs de débrouillage appelés "control word".

Les systèmes existants utilisent des récepteurs qui interrogent leurs modules de sécurité, et ceux-ci répondent en fournissant les informations nécessaires au débrouillage. A un temps donné, pour la même émission diffusée, tous les modules de sécurité répondent la même information. Du fait que les informations circulant entre le module de sécurité et le récepteur sont de faible débit (de l'ordre de 20 à 30 Octets/sec), des fraudeurs peuvent utiliser ces informations pour les diffuser publiquement, par exemple par le biais d'Internet.

Le problème se pose alors de rendre interdépendants un récepteur et un module de sécurité afin que :

- le module de sécurité donné ne puisse être utilisé que dans le récepteur pour lequel le dit module de sécurité a été prévu;
- le flux d'informations échangé entre le module de sécurité et le récepteur soit unique. Cette unicité empêche que la diffusion publique de ce flux permette à d'autres récepteurs de travailler sans le module de sécurité prévu à cet effet.

EXPOSE DE L'INVENTION

La solution proposée aux problèmes cités ci-dessus utilise au moins une clé de chiffrement propre au récepteur. Cette (ou ces) clé(s) est(sont) appelée(s) clé d'appariement. Au moins une des clés est différente pour chaque récepteur. Cette (ou ces) clé(s) est(sont) installée(s) dans la mémoire non volatile du récepteur, soit à la fabrication du dit récepteur, soit à une étape ultérieure. Le récepteur ne fournit au monde extérieur aucun moyen d'accès à cette (ou ces) clé(s).

Un moyen possible pour programmer cette clé dans le module de sécurité est d'utiliser le système d'information central qui gère le parc de récepteurs et qui peut noyer dans le flux de la transmission vidéo des informations pour la programmation de cette clé dans la mémoire non volatile et secrète des modules de sécurité. Le formatage de cette procédure est bien entendu tenu secret.

Lors d'un transfert d'informations sensibles et/ou nécessaires au fonctionnement du système du module de sécurité vers le récepteur (typiquement des "control words", mais d'autres informations peuvent être transférées ainsi), le module de sécurité chiffre ces informations à l'aide d'une ou de plusieurs clés d'appariement uniques, communes au seul couple récepteur/module de sécurité. La méthode de chiffrement est quelconque mais connue du module de sécurité, et le récepteur connaît la méthode de déchiffrement correspondante. Une fois reçues par le récepteur, ces informations sont alors déchiffrées par le dit récepteur en utilisant la méthode de déchiffrement connue et la clé d'appariement

stockée dans sa mémoire non volatile. Les dites informations sont alors en clair et utilisables par le dit récepteur.

L'invention propose donc un système de contrôle de transmission d'informations entre un récepteur et un module de sécurité, notamment pour un système de télévision à péage, où les informations transmises sont chiffrées et déchiffrées au moyen d'au moins une clé de chiffrement unique, stockée d'une part dans le récepteur, et d'autre part dans le module de sécurité.

L'invention concerne également un système de débrouillage d'informations brouillées et un système de télévision à péage comportant un système de contrôle de transmission.

D'autre part, l'invention concerne une méthode de contrôle de transmission d'informations entre un récepteur et un module de sécurité, notamment pour un système de télévision à péage, caractérisé en ce que l'on stocke au moins une clé de chiffrement unique, d'une part dans le récepteur, et d'autre part dans le module de sécurité, et que l'on chiffre et déchiffre les informations transmises entre le récepteur et le module de sécurité au moyen d'au moins une dite clé de chiffrement unique.

Cette solution selon l'invention répond aux problèmes posés. En effet :

- un module de sécurité inséré dans un autre récepteur que celui avec lequel le dit module de sécurité a été apparié fournira à cet autre récepteur un flux d'informations sensibles et/ou nécessaires au fonctionnement du système chiffré avec une clé ne correspondant pas à celle utilisée pour le déchiffrer. Le résultat est alors inutilisable;

- un flux d'informations sensibles et/ou nécessaires au fonctionnement du système provenant d'un module de sécurité ne peut être distribué à plusieurs récepteurs. Seul le récepteur apparié avec la carte fournissant ce flux d'informations sensibles et/ou nécessaire est à même de déchiffrer le dit flux avec succès.

Le système peut comprendre un mécanisme de vérification de l'appariement. Le système d'information central peut inscrire un numéro personnel au récepteur dans le module de sécurité apparié avec le dit récepteur, par exemple généré d'une manière aléatoire par ce dernier, ou simplement utiliser son numéro de série. Un moyen est offert au récepteur de vérifier librement ce numéro personnel inscrit dans le module de sécurité et de le comparer à celui stocké dans sa mémoire non volatile.

Ce mécanisme a l'avantage de ne pas utiliser des données impropres. Le résultat d'un chiffrement suivi d'un déchiffrement par une clé différente fournit usuellement un résultat pseudo-aléatoire. Si le résultat n'est pas reconnu comme faux et que ce résultat est utilisé tel quel, il pourrait en résulter des dommages pour le récepteur ou les appareils connectés à celui-ci.

Certains types de récepteurs comportent un module de débrouillage détachable. Ce module prend en charge un certain nombre d'opérations parmi lesquelles l'opération de débrouillage des signaux reçus. Le transfert d'informations sensibles s'effectue alors entre le module de sécurité détachable et ce module de débrouillage détachable. Le mécanisme de chiffrement de la communication décrit ci-dessus entre un récepteur et un module de sécurité est alors reporté tel quel entre le module de sécurité détachable et le module de débrouillage détachable.

De la même manière, le mécanisme d'appariement décrit ci-dessus entre le module de sécurité et le récepteur est alors reporté tel quel entre le module de sécurité détachable et le module de débrouillage détachable.

Un transfert de signaux débrouillés s'effectue alors entre le module de débrouillage détachable et le récepteur. Le mécanisme de chiffrement de la communication de même que le mécanisme d'appariement décrit ci-dessus, entre le module de sécurité et le récepteur, est alors reporté tel quel entre le récepteur et le module de débrouillage détachable.

Les fonctions assurées par le module de débrouillage détachable et le module de sécurité détachable peuvent être exécutées par un seul module appelé module de débrouillage et de sécurité détachable. Le mécanisme d'appariement précédemment décrit est alors reporté tel quel entre le module de débrouillage et de sécurité détachable et le récepteur.

Dans tous les cas décrits ci-dessus, la ou les clés d'appariement peuvent être utilisées pour chiffrer un flux de données sensibles et/ou nécessaires au fonctionnement du système dans le sens opposé, en intervertissant respectivement :

- récepteur et module de sécurité détachable;
- module de débrouillage détachable et module de sécurité détachable ;
- récepteur et module de débrouillage détachable;
- récepteur et module de débrouillage et de sécurité détachable.

Dans tous les cas où une clé d'appariement est propre à un appareil (récepteur ou module détachable), les mêmes principes s'appliquent à l'utilisation d'une (ou de plusieurs) clé(s) d'appariement propre(s) à un groupe d'appareils.

BRÈVE DESCRIPTION DES FIGURES

La Figure 1 illustre une configuration mettant en œuvre un récepteur et un module de sécurité détachable.

La Figure 2 illustre une configuration mettant en œuvre un récepteur, un module de débrouillage détachable et un module de sécurité détachable.

La Figure 3 illustre une configuration mettant en œuvre un récepteur et un module de débrouillage et de sécurité détachable.

DESCRIPTION DETAILLEE

Le récepteur A de la Figure 1 reçoit un flux d'informations vidéo brouillées 1 d'une source telle qu'un récepteur satellite ou par câble. Ce flux, de l'ordre de plusieurs Megabits par seconde est mis en forme dans le récepteur A puis transmis à une unité de contrôle B qui est responsable du débrouillage et de la gestion de l'autorisation d'accès aux informations vidéos brouillées. Pour ce faire, cette unité de contrôle B interroge périodiquement le module de sécurité détachable C (canal 3) lequel répond à celui-ci par un flux de données sensibles et/ou nécessaires au fonctionnement de l'unité de contrôle B (canal 4). Ces échanges se font à des débits faibles et peuvent être facilement traités par les microprocesseurs des cartes intelligentes disponible sur le marché. Selon l'invention, le module de sécurité détachable C comprend au moins une clé de chiffrement K dans une mémoire non volatile grâce à laquelle sont chiffrées les données sensibles et/ou nécessaires au fonctionnement de l'unité de contrôle B (canal 4) vers le récepteur A. Cette clé K est unique au récepteur A et inscrite au module de sécurité détachable C, rendant le flux d'informations 4 unique à cet ensemble. La diffusion publique de ces informations 4 ne sera plus d'aucune utilité à d'autres récepteurs car pour ces derniers, n'étant pas en possession de la même clé K, le flux d'informations est parfaitement incompréhensible. Au moyen des informations 4, l'unité de contrôle B peut retrouver le signal vidéo débrouillé 2, celui-ci étant traité puis transmis sous une forme standard (PAL, SECAM, NTSC) au moniteur vidéo.

Une variante de l'invention met en œuvre un chiffrement de même nature des informations 3 envoyées au module de sécurité détachable C soit par la même clé K, soit par une clé différente J, unique et propre à l'ensemble formé par le récepteur A et le module de sécurité détachable C. Ainsi, toute tentative visant à retrouver la clé K du flux d'informations 4 est rendue beaucoup plus difficile.

La Figure 2 illustre une variante utilisant un module de débrouillage détachable D intégrant l'unité de contrôle B. Dans ce cas, le flux vidéo

brouillé 1 est mis en forme par le récepteur A et acheminé vers le module de débrouillage détachable D. Le mode de fonctionnement décrit pour la Figure 1 entre le récepteur A et le module de sécurité détachable C est cette fois appliqué au dialogue entre le module de débrouillage détachable D et le module de sécurité détachable C. Le clé K est inscrite dans une partie secrète du module de débrouillage détachable D en lieu et place du récepteur A. Ainsi, les informations fournies par le module de sécurité détachable C au module de débrouillage détachable D sont chiffrées et donc sans valeurs pour un autre module de débrouillage détachable D.

On constate alors que les informations transmises au récepteur A constitue en un flux d'informations vidéos débrouillées 6 et qui peuvent être facilement exploitables, pour des copies illicites par exemple. Dans une variante de l'invention, le flux 6 est chiffré dans le module de débrouillage détachable D avant d'être transmis au récepteur A pour déchiffrage par l'unité de déchiffrement E'. Cette opération est effectuée par une clé K' propre uniquement à l'ensemble récepteur A et au module de débrouillage détachable D. De ce fait, le flux d'informations 6 n'a plus aucune signification et ne peut être compris que par le récepteur A disposant de la même clé K'.

Dans le flux vidéo brouillé 1, le récepteur A peut y adjoindre des informations de contrôle à destination du module de débrouillage détachable D. Afin d'éviter que ces informations soient publiques et ouvre une porte à la compréhension du mécanisme de chiffrement, ces informations sont chiffrées par l'unité de chiffrement E pour obtenir un flux vidéo brouillé 6 contenant des informations de contrôle chiffrées.

La Figure 3 illustre une variante de l'invention où le module de sécurité détachable est intégré dans un module de débrouillage et de sécurité détachable F. Ce module a pour fonction de débrouiller et de gérer l'autorisation des signaux vidéos reçus par le récepteur A. Selon l'invention, ce module comprend une clé unique de chiffrement, propre au

récepteur A et inscrite dans ce module de débrouillage et de sécurité détachable F. De cette manière, le flux vidéo débrouillé 6 est chiffré par cette clé et transmis sous cette forme au récepteur A. Celui-ci, grâce à l'unité de déchiffrement E', et en utilisant la même clé unique, pourra retrouver le signal vidéo en clair.

Par analogie au fonctionnement décrit à la Figure 2, les informations de contrôle contenues dans le flux de vidéo brouillé 1 peuvent être chiffrées au moyen d'une clé unique de chiffrement par l'unité E avant leur transmission vers le module de débrouillage et de sécurité détachable F.

Dans tous les exemples décrit dans les Figures 1 à 3, le contrôle de l'appariement peut s'effectuer. Dans le cas de la Figure 1, le récepteur A inscrit un numéro personnel, par exemple son numéro de série, dans le module de sécurité détachable C. Ainsi, le récepteur peut à tout instant, vérifier que le module de sécurité détachable C est bien celui qui lui est destiné. Dans le cadre de l'exemple illustré à la Figure 2, le contrôle peut se faire à deux niveaux: un premier niveau entre le module de débrouillage détachable D et le module de sécurité détachable C; et un deuxième niveau entre le module de débrouillage détachable D et le récepteur A. Ce deuxième niveau est particulièrement important si l'on chiffre les informations débrouillées 6 en direction du récepteur A.

Dans la solution de la Figure 3, le contrôle de l'appariement s'effectue entre le récepteur A et le module de débrouillage et de sécurité détachable F.

Dans une forme particulière de l'invention, le récepteur A est un décodeur MPEG utilisant des "control words" (informations nécessaires au débrouillage du signal) pour le débrouillage du signal vidéo. Ces "control words" sont fournis par le module de sécurité détachable C. Ce module, par exemple une carte à puce intelligente, comprend une mémoire non volatile pour leur stockage.

Dans une forme particulière de l'invention, le module de débrouillage détachable D est une carte de type PCMCIA incluant un décodeur MPEG (unité de contrôle B).

Dans une forme particulière de l'invention, le module de débrouillage et de sécurité détachable F est réalisé sous forme d'une carte à puce intelligente intégrant un décodeur MPEG et un module de sécurité C'.

Dans une forme particulière de l'invention, la clé unique de chiffrement K est commune à un groupe de récepteur. Cette possibilité est intéressante, par exemple, dans une école disposant de plusieurs récepteurs auxquels l'on va appliquer le même module de sécurité détachable suivant les besoins. De la même manière, plusieurs modules de sécurité détachable incluent la même clé de chiffrement pour pouvoir être placés dans n'importe lequel des récepteurs du groupe. Dans ce cas, le contrôle d'appariement se fait sur un numéro qui n'est plus propre à un récepteur mais à un groupe de récepteur. Une combinaison peut être réalisée avec un numéro composé de deux parties, l'une qualifiant le groupe, l'autre qualifiant le récepteur. L'unicité du numéro personnel est respectée, le test de conformité d'appariement se faisant alors plus que sur la partie groupe de ce numéro.

REVENDICATIONS

1. Système de contrôle de transmission d'informations entre un récepteur (A) et des moyens de sécurité (C, D, F), notamment pour un système de télévision à péage, caractérisé en ce qu'au moins une partie des informations (4, 6) transmises des moyens de sécurité (C, D, F) vers le récepteur (A) sont chiffrées par une clé de chiffrement unique.

2. Système de contrôle de transmission d'informations selon la revendication 1, caractérisé en ce que la clé unique de chiffrement est commune à un groupe de récepteurs.

3. Système de contrôle de transmission d'informations selon les revendications 1 ou 2, caractérisé en ce qu'au moins une partie des informations (3, 5) transmises du récepteur (A) vers les moyens de sécurité (C, D, F) sont chiffrées par une clé de chiffrement unique.

4. Système de contrôle de transmission d'informations selon les revendications 1 à 3, caractérisé en ce que le récepteur (A) comprend un numéro personnel qui peut être inscrit dans les moyens de sécurité (C, D, F), ledit récepteur (A) pouvant vérifier à tout moment la conformité de ce numéro personnel inscrit dans lesdits moyens de sécurité (C, D, F).

5. Système de contrôle de transmission d'informations selon la revendication 4, caractérisé en ce que le numéro personnel comporte une partie propre à un groupe de récepteurs et une partie propre à un récepteur, et que la vérification de la conformité de l'appariement s'effectue sur la partie propre au groupe de récepteur.

6. Système de contrôle de transmission d'informations selon les revendications 1 à 5, caractérisé en ce que le récepteur (A) comprend une unité de contrôle (B) et que les moyens de sécurité sont constitués par un module de sécurité détachable (C) dans lequel les informations sensibles et/ou nécessaires (4) au fonctionnement de l'unité de contrôle (B) sont stockées.

7. Système de contrôle de transmission d'informations selon les revendications 1 à 5, caractérisé en ce que les moyens de sécurité comprennent un module de débrouillage et de sécurité détachable (F) comprenant une unité de contrôle (B) et une unité de sécurité (C') responsables du débrouillage et de l'autorisation des informations vidéos.

8. Système de contrôle de transmission d'informations entre un récepteur (A) et des moyens de sécurité (C, D, F), notamment pour un système de télévision à péage, caractérisé en ce que ces moyens de sécurité comprennent un module de sécurité détachable (C) et un module de débrouillage détachable (D) incluant une unité de contrôle (B), et en ce qu'au moins une partie des informations sensibles et/ou nécessaires (4) au fonctionnement de l'unité de contrôle (B) sont chiffrées avant d'être transmises au module de débrouillage détachable (D) par le module de sécurité détachable (C) au moyen d'une clé de chiffrement unique.

9. Système de contrôle de transmission d'informations selon la revendication 8, caractérisé en ce qu'au moins une partie des informations (3) transmises du module de débrouillage détachable (D) vers le module de sécurité (C) sont chiffrées par une clé de chiffrement unique.

10. Système de contrôle de transmission d'informations selon les revendications 8 ou 9, caractérisé en ce que le module de débrouillage détachable (D) comprend un numéro personnel qui peut être inscrit dans le module de sécurité détachable (C), ledit module de débrouillage détachable (D) pouvant vérifier à tout moment la conformité de ce numéro personnel inscrit dans ledit module de sécurité détachable (C).

11. Système de contrôle de transmission d'informations selon la revendication 10, caractérisé en ce que le numéro personnel comporte une partie propre à un groupe de modules de débrouillage détachables (D) et une partie propre à un module de débrouillage détachable (D), et que la vérification de la conformité de l'appariement s'effectue sur la partie propre au groupe de modules de débrouillage détachables (D).

12. Système de contrôle de transmission d'informations selon les revendications 9 à 11, caractérisé en ce qu'au moins une partie des informations (5) transmises du récepteur (A) vers le module de débrouillage détachable (D) sont chiffrées par une clé de chiffrement unique.

13. Système de contrôle de transmission d'informations selon les revendications 9 à 12, caractérisé en ce qu'au moins une partie des informations (6) transmises du module de débrouillage détachable (D) vers le récepteur (A) sont chiffrées par une clé de chiffrement unique.

14. Système de contrôle de transmission d'informations selon les revendications 12 à 13, caractérisé en ce que le récepteur (A) comprend un numéro personnel qui peut être inscrit dans le module de débrouillage détachable (D), ledit récepteur (A) pouvant vérifier à tout moment la conformité de ce numéro personnel inscrit dans ledit module de débrouillage détachable (D).

15. Méthode de contrôle de transmission d'informations entre un récepteur (A) et des moyens de sécurité (C, D, F), notamment pour un système de télévision à péage, caractérisé en ce que l'on stocke au moins une clé de chiffrement unique, d'une part dans le récepteur (A), et d'autre part dans les moyens de sécurité, et que l'on chiffre et déchiffre les informations transmises entre le récepteur (A) et les moyens de sécurité au moyen d'au moins une des dites clés de chiffrement unique.

16. Méthode selon la revendication 15, caractérisé en ce qu'un numéro personnel au récepteur (A) est inscrit dans les moyens de sécurité lors d'une opération d'initialisation et que le récepteur (A) peut contrôler à tout moment la conformité de ce numéro personnel inscrit dans lesdits moyens de sécurité.

17. Module de sécurité détachable (C) destiné à être connecté à un récepteur (A) comme partie d'un système de télévision à péage, comprenant au moins une mémoire non volatile destinée au stockage des

données sensibles et/ou nécessaires au fonctionnement du système de débrouillage, des moyens de transmission avec le récepteur (A), caractérisé en ce que ce module de sécurité détachable (C) comprend des moyens de chiffrement de la transmission, et que cette mémoire comprend également au moins une clé de chiffrement agissant sur les moyens de chiffrement de la transmission.

18. Module de débrouillage détachable (D) comprenant une unité de contrôle (B), des premiers moyens de transmission (3, 4) avec un module de sécurité détachable (C), des deuxièmes moyens de transmission (5, 6) avec un récepteur (A), ainsi qu'une mémoire non volatile, caractérisé en ce qu'il comprend des premiers moyens de chiffrement, et que cette mémoire comprend au moins une clé de chiffrement agissant sur les premiers moyens de chiffrement destinés à chiffrer la transmission des premiers moyens de transmission (3, 4).

19. Module de débrouillage détachable (D) selon la revendication 18, caractérisé en ce qu'il comprend des deuxièmes moyens de chiffrement, et que cette mémoire comprend au moins une clé de chiffrement agissant sur les deuxièmes moyens de chiffrement destinés à chiffrer la transmission des deuxièmes moyens de transmission (5, 6).

20. Récepteur de débrouillage pour télévision à péage (A) comprenant des moyens de transmission vers des moyens de sécurité (C, D, F), ainsi qu'une mémoire non volatile, caractérisé en ce qu'il comprend des moyens de chiffrement de la transmission de et vers les moyens de sécurité (C, D, F) et que cette mémoire comprend au moins une clé de chiffrement agissant sur les moyens de chiffrement de la transmission.

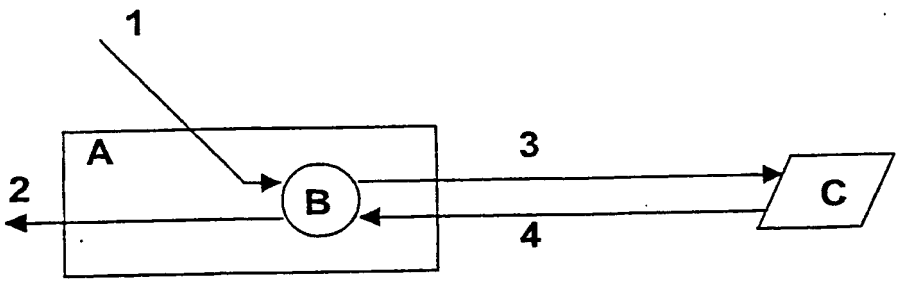


Fig. 1

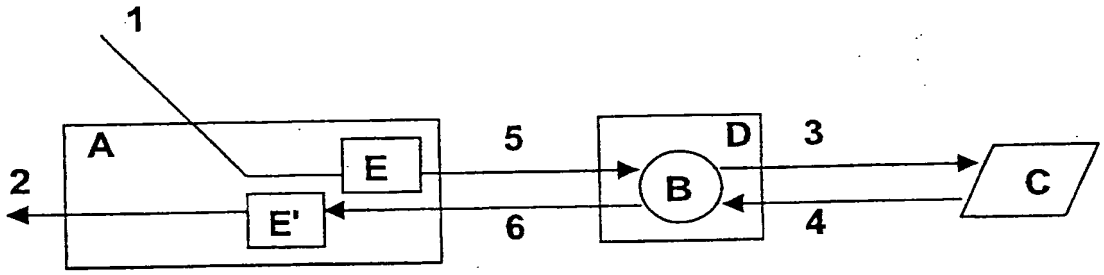


Fig. 2

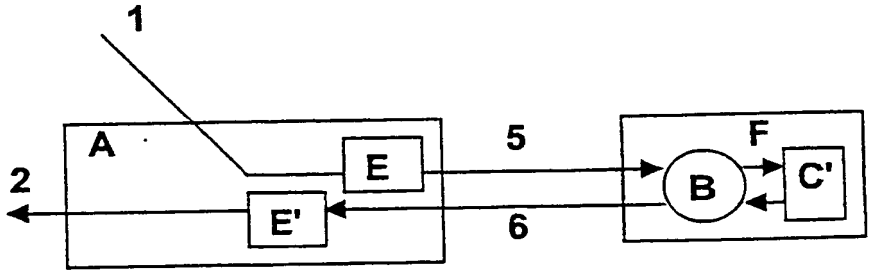


Fig. 3

INTERNATIONAL SEARCH REPORT

National Application No
PCT/IB 99/00821

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04N7/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CUTTS D J: "DVB CONDITIONAL ACCESS" ELECTRONICS AND COMMUNICATION ENGINEERING JOURNAL, vol. 9, no. 1, 1 February 1997, pages 21-27, XP000722905	1,8,15, 17,18,20
A	see the whole document	2-7, 9-14,16, 19

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 June 1999	05/07/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl. Fax: (+31-70) 340-3016	Greve, M

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

	ıational Application No
	PCT/IB 99/00821

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropnate, of the relevant passages	Relevant to claim No.
Y	WRIGHT D T: "CONDITIONAL ACCESS BROADCASTING: DATACARE 2. AN OVER-AIR ENABLED SYSTEM FOR GENERAL PURPOSE DATA CHANNELS" BBC RESEARCH AND DEVELOPMENT REPORT, no. 10, 1 August 1988, pages 1-18, XP000577263	1,8,15, 17,18,20
A	see page 6, right-hand column, line 32 - line 36	2-7, 9-14,16, 19
A	BUER M ET AL: "INTEGRATED SECURITY FOR DIGITAL VIDEO BROADCAST" IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, vol. 42, no. 3, 1 August 1996, pages 500-503, XP000638531 see the whole document	1-20
A	WO 97 38530 A (DAVIES DONALD WATTS ;GLASSPOOL ANDREW (GB); DIGCO B V (NL); RIX SI) 16 October 1997 see the whole document	1-20

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Ir ational Application No
PCT/IB 99/00821

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9738530 A	16-10-1997	AU 2506397 A	29-10-1997
		CA 2250833 A	16-10-1997
		EP 0891670 A	20-01-1999
		HR 970160 A	28-02-1998

RAPPORT DE RECHERCHE INTERNATIONALE

ande Internationale No
PCT/IB 99/00821

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 H04N7/16

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 6 H04N

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	CUTTS D J: "DVB CONDITIONAL ACCESS" ELECTRONICS AND COMMUNICATION ENGINEERING JOURNAL, vol. 9, no. 1, 1 février 1997, pages 21-27, XP000722905	1,8,15, 17,18,20
A	voir le document en entier	2-7, 9-14,16, 19

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
24 juin 1999	05/07/1999

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040. Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Greve, M

1

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/IB 99/00821

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	WRIGHT D T: "CONDITIONAL ACCESS BROADCASTING: DATACARE 2. AN OVER-AIR ENABLED SYSTEM FOR GENERAL PURPOSE DATA CHANNELS" BBC RESEARCH AND DEVELOPMENT REPORT, no. 10, 1 août 1988, pages 1-18, XP000577263	1,8,15, 17,18,20
A	voir page 6, colonne de droite, ligne 32 - ligne 36	2-7, 9-14,16, 19
A	BUER M ET AL: "INTEGRATED SECURITY FOR DIGITAL VIDEO BROADCAST" IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, vol. 42, no. 3, 1 août 1996, pages 500-503, XP000638531 voir le document en entier	1-20
A	WO 97 38530 A (DAVIES DONALD WATTS ;GLASSPOOL ANDREW (GB); DIGCO B V (NL); RIX SI) 16 octobre 1997 voir le document en entier	1-20

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relati. aux membres de familles de brevets

Demande internationale No
PCT/IB 99/00821

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 9738530 A	16-10-1997	AU 2506397 A	29-10-1997
		CA 2250833 A	16-10-1997
		EP 0891670 A	20-01-1999
		HR 970160 A	28-02-1998